REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-34 are pending in the application. The Examiner additionally stated that claims 1-34 are rejected. By this communication, claims 1, 10-11, 14, 22, 25-26, and 28 are amended. Hence, claims 1-34 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-5, 10-11, 13-22, 25-28, and 31-34 under 35 U.S.C. 103(a) as being unpatentable over Yup et al., US PGP No. 20020191784 (hereinafter, "Yup"), and further in view of Best, US Patent No. 4,168,396 (hereinafter, "Best"). Applicant respectfully traverses the Examiner's rejections.

As per claims 1, 22, and 28, the Examiner wrote that Yup teaches an apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said one of the cryptographic operations comprises: [see paragraphs 0038-0039]

- a plurality of CFB block cryptographic operations performed on a corresponding plurality of input text blocks; [see paragraph 0040]
- [CFB] mode logic, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to update pointer registers and

intermediate results for each of said plurality of [CFB] block cryptographic operations; and [see paragraph 0025]

- execution logic, operatively coupled to said [CFB) block pointer logic, configured to execute said one of the cryptographic operations. [see paragraph 0041]

The Examiner conceded that Yup is not explicit in teaching CFB block cryptographic operations, but that Yup teaches cryptographic operations on multiple successive blocks of text. The Examiner noted that Yup does not expressly state that these cryptographic operations are of cipher block chaining mode, but that as is evident in Applicant's disclosure on paragraph 0012 of the specification, it is well known that all symmetric key algorithms employ the same types of modes, and that ECB, CBC, CFB, and OFB are examples that Applicant discloses. Based on this, the Examiner deemed it obvious for one of ordinary skill in the art to implement CFB or any other block cipher mode in conjunction with the system/apparatus taught by Yup.

The Examiner also noted that Yup is not explicit in teaching that the computing device is a microprocessor and, for this limitation, the Examiner relies on Best, col. 2, lines 67-68 and col. 3, lines 1-12. The Examiner observed that Best teaches a microprocessor for executing computer programs which have been enciphered during manufacture to deter the execution of programs in unauthorized computers and that this microprocessor deciphers and executes an enciphered program one instruction at a time, through a combination of substitutions, transpositions, and exclusive-OR additions, in which the address of each instruction is combined with the instruction.

The Examiner thus concluded that it would have been obvious at the time of the invention to one of ordinary skill in the art to implement the invention cited above by Yup within a microprocessor, as taught by Best, in order to provided a secure cryptographic system which is suitable for protecting programs which are deciphered one byte at a time as the program executes.

In response to Applicant's arguments submitted in the previous communication, the Examiner noted that the arguments were considered, but are moot in view of the new grounds of rejection.

Applicant respectfully disagrees with the Examiner's characterization and understanding of the prior art and the invention as recited in claims 1, 22, and 28. Thus, the following points are submitted in traversal of the rejection.

First, one skilled in the art will concur that a microprocessor includes an understood set of functions and logic elements. Generally speaking, a microprocessor is understood by those in the art to be a programmable digital electronic component that incorporates the functions of a central processing unit (CPU) on a single integrated circuit (IC). The aforementioned aspects of the microprocessor according to the present invention are very adequately disclosed within the instant application to include the ability to fetch and execute instructions that have been provided in an application program, to perform address translation, to load and store variables from/to memory, etc. As such, a microprocessor differs from a coprocessor, which is conventionally understood to supplement the functions of the CPU. Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption, as has been discussed in the instant application. Coprocessors require the host main processor to fetch the coprocessor instructions and handle all other operations aside from the coprocessor functions. Accordingly, and as Applicant has discussed in the instant application and in the previous response, a microprocessor is not a coprocessor, nor is a coprocessor a microprocessor. Applicant has discussed the existence and disadvantages of present day cryptographic coprocessors, and has provided the present invention to overcome the disadvantages of such.

The apparatus of Yup is not even a coprocessor. It is a circuit. And as such, Yup's circuit falls into that class of devices that are employed to offload operations from a host processor, examples of which Applicant discussed in the instant disclosure. Certainly, Yup does not disclose, suggest, allude to, or even hint that his circuit be construed or combined with other circuits to yield a coprocessor, much less a microprocessor.

Applicant wishes to raise several points with regard to the Best disclosure. First and foremost, that which Best refers to as a "microprocessor" is a device which is over thirty years old. As the Examiner has written in the instant office action, Best's microprocessor

deciphers and executes an enciphered program one instruction at a time (Abstract). That is, it fetches an instruction from memory, deciphers it, and executes it. Then it fetches a next instruction. And so on.

In contrast, Applicant has amended claims 1, 23, and 30 to recite a "pipeline microprocessor" as is disclosed in numerous places in the instant specification. That is, the present invention is a processor that comprises a plurality of stages (e.g., fetch stage, translate stage, address stage, execute stage, writeback stage), which--during the same clock cycle--are executing operations on a corresponding number of program instructions.

Accordingly, it is respectfully submitted that the limitation of a "pipeline microprocessor" sufficiently distinguishes the present invention over the teachings of Best. Best does not contemplate a microprocessor comprising a plurality of stages because such a concept had not even been conceived at the time of invention.

In another respect, Applicant asserts that Best teaches away from the use of a microprocessor to perform "a plurality of CFB block cryptographic operations," as is recited in each of the independent claims. More specifically, Best notes that a "deciphering processor using such a block cipher is highly secure, *but is complex, costly and slow* for the kind of microcomputers contemplated for use with the present invention." (col. 1, line 67 – col. 2, line 3) In addition, Best also states that the "purpose of making each cipher a function of its address is to avoid the weaknesses of monoalphabetic substitution and *the slowness of a block cipher*." (col. 3, lines 9-12) And Best notes that "[p]rior-art inventions based on the teachings of Feistel previously referenced *are complex and slow* because they require the use of a variable cipher key, publicly known substitution functions, and many transposition and substitution steps," and "[a] different approach is used in the present invention. Since the microprocessor will be used only with the enciphered programs which are authorized for it, a variable key is not essential. Since different substitution functions will be used for each software system or perhaps each unit, the details of the substitution functions may be kept secret, even though the general design is publicly known. By using the system design herein

disclosed, the deciphering step can be done in one clock cycle, so that execution is not slowed by the deciphering process." (col. 3, lines 13-27)

In another place Best points out that the "substitution/transposition/substitution (STS) system in FIG. 3 *does not contain enough steps for a secure block cipher."* (col. 9 lines 50-52)

It is indisputable, then, that Best does anything other than teach away from the solution provided by the present invention. Clearly, one skilled in the art would understand Best to teach that the performance of block cryptographic operations, as is recited in each of the independent claims, is a capability that cannot be attributed to a microprocessor, much less to a pipeline microprocessor.

And, taken alone, Yup's disclosure would point one skilled in the art toward a special circuit, perhaps a coprocessor approach, to performing AES rounds.

Finally, it is submitted that Best's microprocessor does not perform encryption of any sort, which is recited in three of the dependent claims.

Thus, combining the teachings of Yup and Best, one skilled in the art would be led to implement Yup's special circuit to perform AES block cipher operations as an adjunct to Best's "microprocessor," for Best clearly states his approach is not applicable for block cipher operations, because they are too complex and slow to execute.

Accordingly, it is respectfully requested that the rejections of claims 1, 22, and 28 be withdrawn.

With respect to claims 2-5, 10-11, and 13-21, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-5, 10-11, and 13-21.

With respect to claims 25-27, these claims depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 25-27.

With respect to claims 31-34, these claims depend from claim 28 and add further limitations that are neither anticipated nor made obvious by Yup, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 31-34.

The Examiner also rejected claims 6-9, 12, 23-24, and 29-30, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yup and Best as applied to claim 1 above, and further in view of Sorimachi et al., US Patent No. 7184549.

Applicant respectfully traverses the rejections and notes that 6-9, 12, 23-24, and 29-30 depend from claims 1, 22, and 28, as appropriate, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, it is requested that the rejections of claims 6-9, 12, 23-24, and 29-30 be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-34 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/ Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

07/19/2008

Date: _____